Libertés ou sécurités ?

Poullet, Yves

Published in:
Revue Ubiquité. Droit des technologies de l'information

Publication date:
2002

Document Version
le PDF de l'éditeur

ÉDITORIAL

Libertés ou sécurité ?

Yves POULLET[1]

L'adversaire d'une vraie liberté est un désir excessif de sécurité.
Jean de la Fontaine

A la question : « Etes-vous prêts à sacrifier vos libertés pour plus de sécurité ? », les sondages indiquent que la catastrophe du 11 septembre 2001 incite la majorité des citoyens à répondre positivement. Il s'impose de rappeler à une telle majorité le mot du président Thomas Jefferson : « Si tu es prêt à sacrifier un peu de liberté pour te sentir en sécurité, tu ne mérites ni l'une, ni l'autre ».

Forts de cette opinion relayée et amplifiée par les médias, les pouvoirs politiques préparent dans la hâte, tant au niveau national qu'européen, des législations accroissant les pouvoirs des autorités judiciaires et policières afin de mener une lutte efficace contre la cybercriminalité. Osera-t-on leur rappeler que les bandes de Ben Laden, à supposer qu'elles soient coupables des événements du 11 septembre, ne semblent point avoir eu besoin des vertus de l'internet pour commettre leur crime ?

Que disent ces législations écrites à la diable ? Elles obligent les divers fournisseurs de services de communications électroniques privées ou publiques à conserver pendant un délai fixé par d'aucuns à un an (la législation belge établit qu'il s'agit là d'un délai minimal !) les données qui résultent de notre utilisation de ces services. On crée des données sur toute la population à des fins préventives de lutte contre la criminalité, sans soupçon concret.

Un tel prescrit laisse imaginer sans peine l'ampleur de la tâche de ceux qui devront s'y atteler. La liste des prestataires de services de communication s'allonge à l'infini lorsqu'on songe, d'une part, aux multiples réseaux (mobiles, TV, téléphone, intranet) qu'empruntent les communications et, d'autre part, à l'infinité des prestataires qui y opèrent. Les données susceptibles d'être stockées sont infinies (outre les données d'identification et de localisation, la durée des connexions, la longueur et les caractéristiques du message, le cas échéant les sites visités, etc.). C'est que l'utilisation de plus en plus intensive des moyens de communication qui témoigne de nos relations, de nos déplacements, de nos goûts, etc., laisse chez tous ces intervenants des traces de plus en plus nombreuses, en des lieux certes disparates, mais susceptibles d'être reliées grâce aux vertus des réseaux et de systèmes de plus en plus performants de traitement de l'information.

1 Professeur aux FUNDP

La simple existence de tels fichiers crée en toute hypothèse des risques de dérive : les prestataires contraints à un tel stockage peuvent être tentés de rentabiliser leurs prestations à d'autres fins. Au-delà de la sécurisation de leurs propres services ou réseaux, on songe au profilage des utilisateurs à des fins propres ou de commercialisation.

Confier la gestion de tels fichiers à des tiers spécialisés en conservation, *a fortiori* aux autorités policières, c'est substituer au risque décrit celui, plus grand encore, de « fichiers mammouths » où toutes les interconnexions deviennent possibles.

Si la Cour européenne des droits de l'homme considère que le seul stockage de données à des fins policières est déjà une atteinte à nos libertés (arrêts *Rotaru, Ammann, …*), les conséquences des traitements de données induits par les législations évoquées ci-dessus appellent des précautions bien plus grandes encore. En effet, on peut craindre que les forces de police puiseront dans ces vastes réservoirs de données les premiers éléments de leur enquête, avant même toute autre investigation (repérage des personnes à proximité du lieu de commission de l'infraction, liste des correspondants, dernier appel entrant ou sortant). Pire, elles peuvent être tentées d'y trouver les moyens d'une surveillance exploratoire de groupes dits « à risque », ceux qui furètent tel ou tel site, ceux qui se connectent au réseau à partir de tel ou tel endroit, jugé chaud, etc.

Le risque de telles dérives justifie que l'on s'interroge sur la légitimité de l'obligation de conservation de données ! Dans l'arrêt *Klass* de 1978, la Cour européenne des droits de l'homme écrit :

« *… la Cour relève que le législateur national jouit d'un certain pouvoir discrétionnaire (quant au choix des modalités du système de surveillance). La Cour souligne néanmoins que les Etats contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée* ».

Nous vivons dans des Etats de droit et la Convention à laquelle ceux-ci adhèrent impose que ceux qui réclament la conservation des données en démontrent le caractère nécessaire pour l'obtention d'un intérêt supérieur aux libertés ainsi diminuées. Où trouve-t-on de telles justifications ? Les autorités policières apparaissent bien muettes. Interrogées à une réunion d'experts convoqués en novembre 2001 par la Commission européenne, elles s'avéraient incapables de présenter autre chose que des opinions et faits divers là où des études statistiques, sociales et psychologiques auraient pu démontrer qu'effectivement, la préparation active de crimes graves passe par l'utilisation de moyens de communication et qu'effectivement, le travail d'investigation exige l'accès rapide aux données d'une telle utilisation. La confrontation avec les fournisseurs de services a, au contraire, révélé l'imprécision des demandes, leur tâtonnement et la rareté de l'efficacité de telles démarches.

A défaut de telles démonstrations, il y a lieu de craindre que le surveillé, « l'ennemi », devienne, selon le mot de M. Cappato, député européen, rapporteur au

Parlement en cette matière, « le simple citoyen qui surfe sur le net ou qui passe un coup de téléphone ».

Poussons le raisonnement jusqu'à l'absurde : tirera-t-on du fait qu'il semble que ceux qui ont opéré les attentats du 11 septembre dernier disposaient de lames de rasoir, la conséquence de la nécessité du fichage de tout acheteur de telles lames ?

La gravité du crime est évoquée pour justifier de telles atteintes. On s'interroge. Y a-t-il un lien fort et nécessaire entre le moyen mis à la disposition de l'autorité policière et la découverte des délinquants ? Non… Par contre, on y verra le moyen aisé du traçage d'autres délits bien plus mineurs et directement liés à l'utilisation des technologies de communication. Par exemple la violation de droits d'auteur à propos d'œuvres présentes sur le net, les tentatives de *hacking*, etc. Mais que penser alors d'un discours qui agite le spectre terroriste pour en réalité l'atteindre une autre cible : celle de délits économiques dont la recherche des auteurs n'apparaît pas justifier le recours aux moyens extraordinaires prévus ?

Les règles de proportionnalité, de nécessité, de prévisibilité et de légalité des mesures qui restreignent nos droits et libertés fondamentaux conduisent en toute hypothèse à exiger que la loi précise les limites strictes de la durée de conservation, qu'elle définisse les données d'identification concernées (les seules données de connexion de l'utilisateur et du moment de la « transaction » ne suffisent-elles pas ?) et circonscrive le devoir de conservation à quelques prestataires de services obligés : ceux qui fournissent l'accès aux réseaux.

Sans doute, même avec de telles limites clairement affirmées au départ, on craindra que la loi à peine votée ne voie progressivement son champ élargi. Depuis la première loi belge sur les repérages de communications, cinq autres lois ont suivi, élargissant chaque fois davantage les atteintes des autorités policières au secret des communications. Ainsi, dira-t-on, puisque de tels réservoirs de données existent, ne peut-on y recourir plus largement ? Cette tendance à ajouter des exceptions aux exceptions, inquiète. Comment, sur ce point, ne pas louer la « sagesse » américaine du *Patriot Act* qui limite à l'horizon de quatre ans, les mesures exceptionnelles attentatoires aux libertés qui y sont contenues ? On ajoutera que, parmi ces mesures, l'obligation de conserver les données n'est même pas reprise.

Parmi les premières réactions négatives à cette mesure, les avocats ont souligné le danger que représentaient pour eux les atteintes ainsi facilitées au secret professionnel. L'autorité policière aura en effet quelques difficultés à démêler *a priori* parmi toutes les communications dont elle ordonnera le relevé, celles couvertes par le secret et les autres.

Enfin, on rappellera que le renforcement de la cybersurveillance exige son contrôle par une autorité indépendante. Est-on sûr que le contrôle des investigations menées sur le terrain par des équipes policières bien entraînées sera effectif, que les autorités judiciaires ou spécifiques de contrôle pourront toujours saisir la portée des utilisations faites des moyens nouveaux d'investigation ? En outre, la circulation d'informations au sein de réseaux de collaboration internationaux ou européens n'exige-t-elle pas un renforcement des contrôles démocratique ou juridictionnel d'Europol, d'Interpol, du futur Eurojust ou d'Enfopol ?

Mais, objectera-t-on aux défenseurs des libertés, quel luxe de précautions. L'homme honnête n'a rien à craindre de cette surveillance mieux assurée qui débusque les méchants et n'effraie pas le gentil. Certains iront même jusqu'à évoquer le mérite de cette surveillance qui force à adopter un comportement toujours plus conforme aux normes sociales.

A ceux-là, je répondrai qu'il n'est pire danger que cette cybersurveillance qui traque l'homme dans son intimité et crée chez lui la hantise perpétuelle du dévoilement. « Par un renversement pervers, cette prééminence obsessionnelle du regard (de l'autorité) se fait au nom même de ce qu'elle détruit. Les valeurs derrière lesquelles elle s'abrite sont de haut vol : justice, vérité, liberté, démocratie, respect des lois, civisme, intégrité. Mais qui ne voit que cette vision, décapante parfois, à force d'user les cibles sur lesquelles elle se porte, lime jusqu'à l'os certains principes qui fondent le vivre-ensemble ? Quand la proportionnalité n'est plus respectée entre les moyens que se donne l'investigation et les buts recherchés, la sacralisation de l'investigation et du dévoilement assoit comme légitimité unique le moyen et non plus la cause » (B. Frappat, « La dictature de la transparence », *Etudes*, 1999, 58).

De plus, de telles mesures, qui créent artificiellement un sentiment de sécurité, évitent que ceux qui les prennent s'interrogent sur le pourquoi du crime et les instruments de politique criminelle qui peuvent faire face à cette montée de violence. Tout passe par la criminalisation et la défense de la société, sans interrogation supplémentaire. Or, on le sait, la criminalité finit toujours par se déplacer ou devenir plus violente si on ne s'attaque pas réellement à ses causes.